UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/773,187	01/31/2001	John Steven Langford	AUS920000943US1	4502

7590 07/02/2004

Robert H. Frantz
P.O. Box 23324
Oklahoma City, OK 73123-2334

EXAMINER
DADA, BEEMNET W

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 07/02/2004 3

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/773,187	**Applicant(s)** LANGFORD ET AL.	
	Examiner Beemnet W Dada	**Art Unit** 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 January 2001*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date # 2

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-16 have been examined.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1, 4-6, 9-11, 15 and 16 are rejected under 35 U.S.C. 102(e) as being anticipated by Crosbie, Mark (US Provisional Application 60,210,922).

4. As per claims 1, 6 and 11, Crosbie teaches a method for detecting possible security violations and issues in a computer system related to user ID substituting and switching (i.e., 'SU' ing), said computer system having a log of user ID substitutions and switches, said method comprising the steps of:

providing a set of rules which define conditions of user ID substitutions and switches which are to be considered possible security issues (i.e., repeated number of SU attempts within a certain period of time) [page 30, section: '1. N failed su pattern'];

providing a process adapted to evaluate said log of user ID substitutions and switches according to said set of rules (i.e., monitoring and analyzing su log information to detect security violations) [page 30, section: '1. N failed su pattern' and pages 13-14, section '1. The IDS Engine'];

evaluating said log of user ID substitutions and switches to find any entries in said log which meet one or more defined conditions in said set of rules (i.e., monitoring and analyzing su log information to detect security violations) [page 30, section: '1. N failed su pattern' and pages 13-14, section '1. The IDS Engine']; and

outputting an alert responsive to finding one or more log entries which meet said conditions [page 13 last and page 14 first line].

5. As per claims 4, 9 and 15, Crosbie teaches the method as applied above. Furthermore, Crosbie teaches, the method, wherein said step of evaluating said log of user ID substitutions and switches comprises evaluating a SULOG file in a system having a UNIX-like operating system (i.e. HP-UX system) [page 9, 2nd and 3rd paragraphs].

6. As per claims 5, 10, 16, Crosbie teaches the method as applied above. Furthermore, Crosbie teaches, the method, wherein said step of outputting an alert comprises sending an electronic message to a predetermined destination address (i.e., sending an alert to a central administrative console) [page 13 last and page 14 first line and page 16 1st paragraph].

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 2, 3, 7, 8, and 12-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Crosbie, Mark (US Provisional Application 60,210,922) in view of Rowland, Craig H (Ref. U).

9. As per claims 2, 3, 7, 8, and 12-14 Crosbie teaches evaluating log of user ID substitutions and switches to find any entries in said log which meet one or more defined conditions in said set of rules (i.e., monitoring and analyzing su log information to detect security violations) [page 30, section: '1. N failed su pattern' and pages 13-14, section '1. The IDS Engine'], in a UNIX-like operating system (i.e. HP-UX system) [page 9, 2nd and 3rd paragraphs]. Furthermore, Crosbie suggests using a daemon to process su log file [page 30 last line].

Crosbie does not explicitly teach evaluating a log by periodically executing a CRON daemon. Rowland teaches a method of detecting security violations comprising evaluating a log by periodically executing a CRON daemon [page 2, 5th paragraph]. Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to evaluate a system log by periodically executing a CRON daemon as per teachings of Rowland and include it into the log monitoring and evaluation method taught by Crosbie, in order to alert violations frequently.

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. PTO Form 892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Beemnet W Dada whose telephone number is (703) 305-8895. The examiner can normally be reached on Monday - Friday (8:30 am - 6:00 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y Vu can be reached on (703) 305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AU 2135

Beemnet Dada

June 17, 2004